Amendments to the Claims:

The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method performed on a device comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider as a first packet;

receiving data indicating that the service provider has verified the signature;

providing one or more tokens to the foreign service provider with a next packet ~~when~~ after the foreign service provider ~~accepts~~ has verified the signature to use the service, wherein the one or more tokens are generated using the hash tree; and

~~continuing to use~~ using the service while the foreign service provider accepts tokens.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) A computer-implemented method performed on a device comprising:

requesting a desired service through a foreign service provider;

generating a dense hash tree and generating a digital signature on a root value of the hash tree, wherein the dense hash tree is constructed by,

randomly generating a number of bit streams equal to the number of tokens that is estimated to be needed,

constructing a binary tree with a number of leaves equal to the number of estimated tokens plus one,

assigning the random bit strings to the leaves, and

computing values to be assigned to each internal node according to the values of children of internal nodes;

sending the digital signature and the root value to the foreign service provider as a first packet;

receiving data indicating that the service provider has verified the signature;

providing one or more tokens to the foreign service provider with a next packet ~~when~~ after the foreign service provider ~~accepts~~ has verified the signature to use the service, wherein the one or more tokens are generated using the hash tree; and

~~continuing to use~~ using the service while the foreign service provider accepts tokens.

5. (Original) The method defined in Claim 4 wherein generating a number of bit streams comprises generating the number of bits streams from a single seed.

6. (Original) The method of Claim 4 wherein the bit strings are of cryptographically suitable length.

7. (Previously Presented) The method of Claim 1 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

8. (Previously Presented) The method of Claim 1 further comprising generating the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

9. (Original) The method of Claim 1 further comprising generating a digital signature on the root of the tree using a private signing key.

10. (Previously Presented) The method of Claim 1 wherein each of the one or more of the tokens includes one or more of a group consisting of the identity of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

11. (Previously Presented) The method of Claim 1 further comprising sending to the foreign service provider a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and a home service provider produced from a private key of the home service provider.

12. (Previously Presented) The method of Claim 1 wherein the one or more tokens is an undeniable token.

13. (Currently Amended) The method of Claim 1 wherein generating the hash tree further comprises:

generating a dense hash tree;

providing the root value to a home service provider for signature; and

transmitting data to ~~informing~~ the home service provider that informs the home service provider of a monetary value of the dense hash tree based on a number of tokens in the dense hash tree, wherein the monetary value of the dense hash tree enables the home service provider to make monetary payments to the foreign service provider based on the one or more tokens provided to the foreign service provider~~; and~~

~~providing payments based on the dense hash tree to the foreign service provider~~.

14. (Currently Amended) An apparatus comprising:

an external network interface through which a request for a desired service of a foreign service provider is made;

a memory;

a processor coupled to the external network interface and the memory, wherein the processor to generate a hash tree and generate a digital signature on a root value of the hash tree using the memory, and further wherein the processor to send the digital signature and the root value to the foreign service provider as a first packet, via the external network interface,

along with one or more tokens with a next packet ~~when~~ after the foreign service provider ~~accepts~~ has verified the signature for use of the service, and ~~continue to~~ use the service while the foreign service provider accepts tokens, wherein the one or more tokens are generated using the hash tree.

15. (Previously Presented) The apparatus of Claim 14 further comprising a user device to generate the one or more tokens.

16. (Previously Presented) The apparatus of Claim 15 wherein the user device to generate tokens using the hash tree.

17. (Original) The apparatus of Claim 16 wherein the hash tree is one selected from a group consisting of a Merkle tree and a dense hash tree.

18. (Previously Presented) The apparatus of Claim 14 wherein the processor to generate the one or more tokens using a public key signature scheme, including using a public-key signature to sign the root of the hash tree.

19. (Original) The apparatus of Claim 14 wherein the processor includes in each of the one or more of the tokens one or more of a group consisting of the identity of the foreign service provider for which tokens are intended, a maximum number of tokens that the foreign service provider may receive, and any conditions that the foreign service provider must satisfy before it can redeem the token.

20. (Previously Presented) The apparatus of Claim 14 wherein the processor causes a signature on the root value of the hash tree, a public key of the user device and a certificate from a trusted party attesting to a relationship between the user and a home service provider, produced from a private key of the home service provider, to the foreign service provider via the external network interface.

21. (Original) The apparatus of Claim 14 wherein the token is an undeniable token.

22. (Currently Amended) The apparatus of Claim 14 wherein to generate a hash tree, the processor provides a root value of a dense hash tree to a home service provider for signature and transmits data that informs the home service provider of a monetary value of the dense hash tree, based on a number of tokens in the dense hash tree, to enable the home service provider to make monetary payments to the foreign service provider for the service based on the one or more tokens sent to the foreign service provider.

23. (Currently Amended) An apparatus comprising:

means for requesting a desired service through a foreign service provider;

means for generating a hash tree and generating a digital signature on a root value of the hash tree;

means for sending the digital signature and the root value to the foreign service provider as a first packet;

means for receiving data indicating that the service provider has verified the signature;

means for providing one or more tokens to the foreign service provider with a next packet ~~when~~ after the foreign service provider ~~accepts~~ has verified the signature to use the service, wherein the one or more tokens are generated using the hash tree; and

means for ~~continuing to use~~ using the service while the foreign service provider accepts tokens.

24. (Currently Amended) An article of manufacture having one or more recordable media storing instructions thereon which, when executed by a system, cause the system to perform a method comprising:

requesting a desired service through a foreign service provider;

generating a hash tree and generating a digital signature on a root value of the hash tree;

sending the digital signature and the root value to the foreign service provider as a first packet;

receiving data indicating that the service provider has verified the signature;

providing one or more tokens to the foreign service provider with a next packet ~~when~~ after the foreign service provider ~~accepts~~ has verified the signature to use the service, wherein the one or more tokens are generated using the hash tree; and

~~continuing to use~~ using the service while the foreign service provider accepts tokens.

25.-54. (Cancelled)